Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers Provided by the U.S. Department of Justice

This appendix provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of computers. The discussion focuses first on the proper way to describe the property to be seized in the warrant itself, which in turn requires consideration of the role of the computer in the offense. The discussion then turns to drafting an accompanying affidavit that establishes probable cause, describes the agent's search strategy, and addresses any additional statutory or constitutional concerns.

1. DESCRIBING THE PROPERTY TO BE SEIZED FOR THE WARRANT

The first step in drafting a warrant to search and seize computers or computer data is to describe the property to be seized for the warrant itself. This requires a particularized description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

Whether the 'property to be seized' should contain a description of information (such as computer files) or physical computer hardware depends on the role of the computer in the offense. In some cases, the computer hardware is itself contraband, evidence of crime, or a fruit or instrumentality of crime. In these situations, Fed. R. Crim. P. 41 expressly authorizes the seizure of the hardware, and the warrant will ordinarily request its seizure. In other cases, however, the computer hardware is merely a storage device for electronic files that are themselves contraband, evidence, or instrumentalities of crime. In these cases, the warrant should request authority to search for and seize the information itself, not the storage devices that the agents believe they must seize to recover the information. Although the agents may need to seize the storage devices for practical reasons, such practical considerations are best addressed in the accompanying affidavit. The 'property to be seized' described in the warrant should fall within one or more of the categories listed in Rule 41(b):

(1) "property that constitutes evidence of the commission of a criminal offense"

This authorization is a broad one, covering any item that an investigator "reasonably could . . . believe" would reveal information that would aid in a particular apprehension or conviction. Andresen v. Maryland, 427 U.S. 463, 483 (1976). Cf. Warden v. Hayden, 387 U.S. 294, 307 (1967) (noting that restrictions on what evidence

may be seized result mostly from the probable cause requirement). The word "property" in Rule 41(b)(1) includes both tangible and intangible property. See United States v. New York Tel. Co., 434 U.S. 159, 169 (1977) ("Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."); United States v. Biasucci, 786 F.2d 504, 509-10 (2d Cir. 1986) (holding that the fruits of video surveillance are "property" that may be seized using a Rule 41 search warrant). Accordingly, data stored in electronic form is "property" that may properly be searched and seized using a Rule 41 warrant. See United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

(2) "contraband, the fruits of crime, or things otherwise criminally possessed"

Property is contraband "when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken." Hayden, 387 U.S. at 302 (quoting Gouled v. United States, 255 U.S. 298, 309 (1921)). Common examples of items that fall within this definition include child pornography, see United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995), pirated software and other copyrighted materials, see United States v. Vastola, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons. The phrase "fruits of crime" refers to property that criminals have acquired as a result of their criminal activities. Common examples include money obtained from illegal transactions, see United States v. Dornblut, 261 F.2d 949, 951 (2d Cir. 1958) (cash obtained in drug transaction), and stolen goods. See United States v. Burkeen, 350 F.2d 261, 264 (6th Cir. 1965) (currency removed from bank during bank robbery).

(3) "property designed or intended for use or which is or had been used as a means of committing a criminal offense"

Rule 41(b)(3) authorizes the search and seizure of "property designed or intended for use or which is or had been used as a means of committing a criminal offense." This language permits courts to issue warrants to search and seize instrumentalities of crime. See United States v. Farrell, 606 F.2d 1341, 1347 (D.C. Cir. 1979). Computers may serve as instrumentalities of crime in many ways. For example, Rule 41 authorizes the seizure of computer equipment as an instrumentality when a suspect uses a computer to view, acquire, and transmit images of child pornography. See Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (stating in an obscenity case that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996). Similarly, a hacker's computer may be used as an instrumentality of crime, and a computer used to run an illegal Internet gambling business would also be an instrumentality of the crime.

Here are examples of how to describe property to be seized when the computer hardware is merely a storage container for electronic evidence:

All records relating to violations of 21 U.S.C. § 841(a)

(drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 1996, including lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 1995 to the present; all bank records, checks, credit card bills, account information, and other financial records.

The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Any copy of the X Company's confidential May 17, 1998 report, in electronic or other form, including any recognizable portion or summary of the contents of that report.

***[For a warrant to obtain records stored with an ISP pursuant to 18 U.S.C. Section 2703(a)]** All stored electronic mail of any kind sent to, from and through the e-mail address [JDoe@isp.com], or associated with the user name "John Doe," or account holder [suspect]. Content and connection log files of all account activity from January 1, 2000, through March 31, 2000, by the user associated with the e-mail address [JDoe@isp.com], including dates, times, methods of connecting (e.g., telnet, ftp, http), ports used, telephone dial-up caller identification records, and any other connection information or traffic data. All business records, in any form kept, in the possession of [Internet Service Provider], that pertain to the subscriber(s) and account(s) associated with the e-mail address [JDoe@isp.com], including records showing the subscriber's full name, all screen names associated with that subscriber and account, all account names associated with*

that subscriber, methods of payment, phone numbers, all residential, business, mailing, and e-mail addresses, detailed billing records, types and lengths of service, and any other identifying information.

Here are examples of how to describe the property to be seized when the computer hardware itself is evidence, contraband, or an instrumentality of crime:

Any computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, Zip disks, and floppy disks) that were or may have been used as a means to provide images of child pornography over the Internet in violation of 18 U.S.C. § 2252A that were accessible via the World Wide Website address www.[xxxxxxxx].com.

IBM Thinkpad Model 760ED laptop computer with a black case

2. DRAFTING AFFIDAVITS IN SUPPORT OF WARRANTS TO SEARCH AND SEIZE COMPUTERS

An affidavit to justify the search and seizure of computer hardware and/or files should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy. In addition, warrants that raise special issues (such as sneak-and-peek warrants, or warrants that may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa) require thorough discussion of those issues in the affidavit. Agents and prosecutors with questions about how to tailor an affidavit and warrant for a computer-related search may contact either the local CTC, or the Computer Crime & Intellectual Property Section at (202) 514-1026.

Background Technical Information

It may be helpful to include a section near the beginning of the affidavit explaining any technical terms that the affiant may use. Although many judges are computer literate, judges generally appreciate a clear, jargon-free explanation of technical terms that may help them understand the merits of the warrant application. At the same time, agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Here are several sample definitions:

Encryption

Encryption refers to the practice of mathematically scrambling computer data as a communications security measure. The encrypted information is called "ciphertext." "Decryption" is the process of converting the ciphertext back into the original, readable information (known as "plaintext"). The word, number or other value used to encrypt/decrypt a message is called the "key."

Data Compression

A process of reducing the number of bits required to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs and most computer data. Other methods do not exactly reproduce the original data, but this may be acceptable (for example, for a video conference).

Joint Photographic Experts Group (JPEG)

JPEG is the name of a standard for compressing digitized images that can be stored on computers. JPEG is often used to compress photographic images, including pornography. Such files are often identified by the ".jpg" extension (such that a JPEG file might have the title "picture.jpg") but can easily be renamed without the ".jpg" extension.

Internet Service Providers ("ISPs")

Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental

storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a "remote computing service."

Server

A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers.

In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

IP Address

The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

> **dynamic IP address** *When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's IP address normally differs each time he dials into the ISP.*

static IP address *A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.*

B. Describe the Role of the Computer in the Offense

The next step is to describe the role of the computer in the offense, to the extent it is known. For example, is the computer hardware itself evidence of a crime or contraband? Is the computer hardware merely a storage device that may or may not contain electronic files that constitute evidence of a crime? To introduce this topic, it may be helpful to explain at the outset why the role of the computer is important for defining the scope of your warrant request.

Your affiant knows that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, the warrant application requests permission to search and seize [images of child pornography, including those that may be stored on a computer]. These [images] constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain [the images of child pornography] if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Your affiant believes that, in this case, the computer hardware is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

1. When the Computer Hardware Is Itself Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

If applicable, the affidavit should explain why probable cause exists to believe that the tangible computer items are themselves contraband, evidence, instrumentalities, or fruits of the crime, independent of the information they may hold.

Computer Used to Obtain Unauthorized Access to a Computer ("Hacking")

Your affiant knows that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the

individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is "used as a means of committing [the] criminal offense" according to Rule 41(b)(3). In particular, the individual's computer is the primary means for accessing the Internet, communicating with the victim computer, and ultimately obtaining the unauthorized access that is prohibited by 18 U.S.C. § 1030. The computer is also likely to be a storage device for evidence of crime because computer hackers generally maintain records and evidence relating to their crimes on their computers. Those records and evidence may include files that recorded the unauthorized access, stolen passwords and other information downloaded from the victim computer, the individual's notes as to how the access was achieved, records of Internet chat discussions about the crime, and other records that indicate the scope of the individual's unauthorized access.

Computers Used to Produce Child Pornography

It is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can be connected to a common video camera using a device called a video capture board: the device turns the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

2. When the Computer Is Merely a Storage Device for Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

When the computer is merely a storage device for electronic evidence, the affidavit should explain this clearly. The affidavit should explain why there is probable cause to believe that evidence of a crime may be found in the location to be searched. This does not require the affidavit to establish probable cause that the evidence may be stored specifically within a computer. However, the affidavit should explain why the agents believe that the information may in fact be stored as an electronic file stored in a computer.

Child Pornography

Your affiant knows that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection.

Illegal Business Operations

Based on actual inspection of [spreadsheets, financial records, invoices], your affiant is aware that computer equipment was used to generate, store, and print documents used in [suspect's] [tax evasion, money laundering, drug trafficking, etc.] scheme. There is reason to believe that the computer system currently located on [suspect's] premises is the same system used to produce and store the [spreadsheets, financial records, invoices], and that both the [spreadsheets, financial records, invoices] and other records relating to [suspect's] criminal enterprise will be stored on [suspect's computer].

C. The Search Strategy

The affidavit should also contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the search strategy as an attachment to the warrant, especially when the affidavit is placed under seal. Here is sample language that can apply recurring situations:

1. Sample Language to Justify Seizing Hardware and Conducting a Subsequent Off-site Search

Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

> *(1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.*
>
> *(2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.*

In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

2. Sample Language to Justify an Incremental Search

Your affiant recognizes that the [Suspect] Corporation is a functioning company with approximately [number] employees, and that a seizure of the [Suspect] Corporation's computer network may have the unintended and undesired effect of limiting the company's ability to provide service to its legitimate customers who are not engaged in [the criminal activity under investigation]. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to [Suspect Corporation]'s legitimate customers and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

> *A. Upon arriving at the [Suspect Corporation's] headquarters on the morning of the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper [and electronic] copies of [the computer files described in the warrant.] If the agents succeed at locating such an employee and are able to obtain copies of the [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.*
>
> *B. If the employees choose not to assist the agents and the agents cannot execute the warrant successfully without themselves examining the [Suspect Corporation's] computers , primary responsibility for the search will transfer from the case agent to a designated computer expert. The computer expert will attempt to locate [the computer files described in the warrant], and will attempt to make electronic copies of those files. This analysis will focus on particular programs, directories, and files that are most likely to contain the evidence and information of the violations under investigation. The computer expert will make every effort to review and copy only those programs, directories, files, and materials that are evidence of the offenses described herein, and provide only those items to the case agent. If the computer expert succeeds at locating [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.*

C. If the computer expert is not able to locate the files on-site, or an on-site search proves infeasible for technical reasons, the computer expert will attempt to create an electronic "image" of those parts of the computer that are likely to store [the computer files described in the warrant]. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The computer expert or another technical expert will then conduct an off-site search for [the computer files described in the warrant] from the "mirror image" copy at a later date. If the computer expert successfully images the [Suspect Corporation's] computers, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

D. If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the [Suspect Corporation's] computer system that the computer expert believes must be seized to permit the agents to locate [the computer files described in the warrant] at an off-site location. The components will be seized and taken in to the custody of the FBI. If employees of [Suspect Corporation] so request, the computer expert will, to the extent practicable, attempt to provide the employees with copies of any files [not within the scope of the warrant] that may be necessary or important to the continuing function of the [Suspect Corporation's] legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

3. Sample Language to Justify the Use of Comprehensive Data Analysis Techniques

Searching [the suspect's] computer system for the evidence described in [Attachment A] may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to

determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in [Attachment A].

Special Considerations

The affidavit should also contain discussions of any special legal considerations that may factor into the search or how it will be conducted. These considerations are discussed at length in Chapter 2. Agents can use this checklist to determine whether a particular computer-related search raises such issues:

1. **Is the search likely to result in the seizure of any drafts of publications (such as books, newsletters, Web site postings, etc.) that are unrelated to the search and are stored on the target computer?** If so, the search may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa.

2. **Is the target of the search an ISP, or will the search result in the seizure of a mail server?** If so, the search may implicate the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-11.

3. **Does the target store electronic files or e-mail on a server maintained in a remote location?** If so, the agents may need to obtain more than one warrant.

4. **Will the search result in the seizure of privileged files, such as attorney-client communications?** If so, special precautions may be in order.

5. **Are the agents requesting authority to execute a sneak-and-peek search?**

6. **Are the agents requesting authority to dispense with the "knock and announce" rule?**

Distributed in Forward Edge II

Sample Affidavit in Support of Search Warrant
Provided by the United States Secret Service

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT APPLICATION

I, [INSERT NAME OF LAW ENFORCEMENT OFFICER], being duly sworn, depose and say:

7. I have been employed as a [INSERT JOB AND AGENCY] for over [INSERT LENGTH OF SERVICE. My current title is [INSERT TITLE].

8. My duties as an agent of the United States Secret Service include the investigation of alleged crimes, including offenses involving the manufacturing of counterfeit obligations of the United States, in violation of Title 18, United States Code, Section 471.

9. My duties as an agent of the United States Secret Service also include that of a Computer Investigative Specialist. I have received extensive training at the Federal Law Enforcement Training Center in the execution of search warrants involving computers and related equipment, electronic data preservation, and the recovery, documentation and authentication of evidence.

10. The following information is known to me personally, or was reported to me by Police Officers with the [INSERT MUNICIPALITY NAME]. Title 18, United States Code, Section 471 makes it an offense for any person, with intent to defraud, to falsely make, forge, counterfeit or alter any obligation or other security of the United States.

Distributed in Forward Edge II

11. On [INSERT DATE], a Search Warrant was obtained to search the home located at [INSERT ADDRESS], the residence of [INSERT NAME], a copy of which Warrant, Application and Affidavit are attached hereto and are incorporated as if fully set out herein. (See Exhibit A).

12. Pursuant to the aforementioned Warrant, a [INSERT DESCRIPTION OF EQUIMENT, WITH SERIAL NUMBERS] were seized as other evidence of forgery.

13. I have reviewed the counterfeit currency detailed in the first Affidavit and it appears that [INSERT DESCRIPTION OF ACTIVITY, such as follows] these counterfeit notes were created using a desktop imaging system. These notes were produced by scanning, copying, modifying or saving an image of a genuine Federal Reserve Note using digital technology. The image of the counterfeit note can then be saved to electronic storage media such as computer disks, diskettes, and CD's. The counterfeit note is then printed using color liquid ink, using an ink jet printer. Ink jet printers spray tiny droplets of ink from the printer head onto the paper to form an image. Counterfeit notes created using these printers can be identified by the tiny multi-colored dot patterns created when the printer uses the ink in an attempt to match the genuine currency colors. Based upon my training and experience, it appears that these notes were created through the use of a computer and were printed on the type of color printer found at the [INSERT ADDRESS] address.

Distributed in Forward Edge II

14. Coupled with information supplied in the original Affidavit and the information set out below, there is probable cause to believe that within that computer there are electronic files and records which will contain evidence of the counterfeiting and forgery.

15. Based on my knowledge, training and experience, I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in three distinct and important respects:

a. The objects themselves may be instrumentalities used to commit the crime.

b. The objects may have been used to collect and store information about crimes (in the form of electronic data).

c. The objects may be contraband or fruits of the crime.

16. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about a crime.

17. Based on my knowledge, training and experience, I know that computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computer); internal and peripheral storage devices (such as fixed disks, external disks, floppy disks drives and diskettes, tape drives and

Distributed in Forward Edge II

tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, communications and optical readers); and related devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic telephone dialing or generating devices), parts that can be dialers, speed dialers, programmable signaling devices, and electronic tones well as any devices, mechanisms, or used to restrict access to computer hardware (such as physical keys and locks).

18. Based on my knowledge, training and experience, I know that computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs (like Internet browsers, electronic mail managers, and Internet relay chat software).

19. Based on my knowledge, training and experience, I know that computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software or other related items.

20. Based on my knowledge, training and experience, I know that computer passwords and other data security devices are designed to restrict access to or hide computer software,

Distributed in Forward Edge II

documentation or data. Data security devices may consist of hardware, software or other programming code. A password (string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software of code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as to reverse the process to restore it.

21. Based on the foregoing facts, my training and experience, I have probable cause to believe that the [INSERT EQUIPMENT] that were recovered from the premises of [INSERT ADDRESS], the residence of [INSERT NAME], have been used to collect, store, maintain, retrieve, and use electronic data in the form of electronic records, documents, and materials. This data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment. This media includes but is not limited to any floppy diskettes, hard drives, backup tapes, CD's, CD-R's, CD-RW's, DVD's, optical discs, or printer buffers, as well as printouts or readouts from any magnetic storage devices.

22. Such electronic data in the form of electronic records, documents, and materials, constitutes evidence of the violation of Title 18, United States Code, Section 471 described in this Affidavit.

Distributed in Forward Edge II

23. Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to the following: examining file directories and subdirectories for the lists of files they contain; "opening" or reading the first few "pages" of selected files to determine their contents; scanning for deleted or hidden data; recovering deleted files; or performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation ("string searches").

24. Based upon the foregoing facts, there is probable cause to believe that [INSERT NAME] has violated 18 U.S.C. 471 by producing (manufacturing) counterfeit Federal Reserve Notes of the United States with intent to defraud and that he used the aforementioned computer and associated devices and media as part of that criminal conduct.

25. Based on the foregoing facts and my training and experience, I have probable cause to believe that evidence of and instrumentalities used to commit this offense are electronically located within [INSERT EQUIPMENT] and the hard drive contained within this computer, that was recovered from [INSERT ADDRESS], the residence of [INSERT NAME].

26. In view of the foregoing, your Affiant respectfully requests that this Court issue a Search Warrant permitting the seizure and search of the property described in Attachment A of this Application and Affidavit for Search Warrant and incorporated herein for all purposes.

Distributed in Forward Edge II

[INSERT OFFICER/AGENT'S NAME].
[INSERT AGENCY]

Sworn to before me and in my

presence this _____ day of

_____, 2003.

_____
HON. [INSERT JUDGE'S NAME]
United States District Judge

Distributed in Forward Edge II

ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

[INSERT EQUIPMENT, such as follows] One Quantex tower computer, serial number 5001796579, including its hard drive, and any other storage devices contained within it, and approximately 87 (eighty seven) computer diskettes and CD=s, which were recovered by Special Agents of the United States Secret Service from the premises of [INSERT ADDRESS], the residence of [INSERT NAME], on [INSERT DATE].

Distributed in Forward Edge II

Affidavit in Support of Search Warrant Sample
(sample details filled in, specifics redacted)
Provided by the United States Secret Service

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE SEARCH OF THE SUN MICROSYSTEMS NETRA MODEL COMPUTER BEARING SERIAL NUMBER 7----5AD; and

THE PREMISES KNOWN AND DESCRIBED AS (ENTER ADDRESS), NORTH BERGEN, NEW JERSEY 07047

TO BE FILED UNDER SEAL

Mag. No. 05- __ MUA

AFFIDAVIT IN SUPPORT

OF SEARCH WARRANT

Robert B. Agent, being duly sworn, deposes and says:

1. I am a Special Agent with the United States Secret Service ("USSS"), assigned to the Electronic Crimes Squad. I have been employed with the USSS since approximately 2000. The Electronic Crimes Squad investigates, among other things, crimes involving the unauthorized intrusion into computers and computer systems, the offense at issue here. Based upon my training as a Secret Service agent and experience to date on the Electronic Crimes Squad, I am familiar with the means by which individuals use computers and information networks to commit various criminal offenses.

2. The information contained in this affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement agents and witnesses, and the review of documents and records. During the course of the investigation, I have become familiar with the item and place to be searched.

3. I submit this affidavit in support of an application for warrants to search:

a. The premises known and described as (Enter Street w/Apartment Number), North Bergen, New Jersey 07047 (hereinafter, the "Apartment"); and

b. The Sun Microsystems Netra model computer bearing serial number

1)
7----5AD (hereinafter, the "Computer"), for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2)(C), which relates to illegally obtaining information from a protected computer through the unauthorized access of that computer.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to search for evidence of violations of 18 U.S.C. § 1030(a)(2)(C). Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

5. Based upon the facts set forth herein, I believe, and respectful1y submit that there is probable cause to believe, that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(2)(C), are located at the Apartment and on the Computer.

THE COMPUTER AND THE APARTMENT

6. The Computer is a Sun Microsystems brand, Netra model computer bearing serial number 7----5AD.

7. The Apartment is apartment number 2, located at (Enter Address), New Jersey 07047. The Apartment is further described as located in a two-family home on the corner of __th Street and 5th Avenue. The ground level is red brick and the upper level is tan stucco. There is also an attic level. There is one entrance to the two-family home on __th Street and is labeled “----" on the door. Another entrance to the two-family home on 5th Avenue has two mailboxes next to it. One mailbox indicates the name "----" and "2ND FLOOR."

Distributed in Forward Edge II

THE INVESTIGATION AND PROBABLE CAUSE
TO SEARCH THE APARTMENT AND THE COMPUTER

8. Other law enforcement agents and I have been involved in an investigation of the unauthorized accessing of a protected computer system of ---------- & Co. ("-----"). Among other things, ----- provides banking services to individuals and businesses, including banking services that it makes accessible by computer.

9. In or about mid-February 2005, another Special Agent of the USSS was contacted by a representative of -----, who himself is a former Special Agent of the USSS. In substance and in part, the ----- representative indicated that there had been an intrusion into -----'s computer network located in New York, New York, and that records for over approximately 20 customer accounts had been accessed by one or more persons not authorized to access these account records and that one of the customer account records had been altered. In addition, the ----- representative informed the other Special Agent of the USSS that the Internet Protocol ("IP") address associated with this unauthorized access was ___.__.___.__.

10. Based on my training and experience, I am aware that the Internet Protocol is the method by which data is sent from computer to computer over the Internet. In general, at any given moment, each computer connected to the Internet has at least one IP address associated with it. Further, at any given moment, an IP address uniquely distinguishes the computer assigned a particular IP address from all other computers connected to the Internet, which are assigned different IP addresses. For a typical user of the Internet, the IP address is assigned to the user's computer by his or her Internet service provider ("ISP").

11. Based on the conversations of another Special Agent of the USSS with a representative of _____.net, I determined that the ISP assigned to ___.__.___.__ is

Distributed in Forward Edge II

_____.net and that, in turn, _____.net assigned this IP address to ---------- LLC ("----------"), an information technology and online services firm located in -------, New Jersey.

12. On or about March 11, 2005, other law enforcement agents, including Special Agents of the USSS, and I spoke with a representative of --------, who informed us that ---------- permitted Dennis ------ to use the IP address ___.__.___.__ since approximately April 2004. The representative of ------- also informed us that Dennis ----- is a friend of one of the founders of ---------- and was lent the IP address ---.--.---.-- for approximately a year. The representative of ---------- also informed us that the only person who uses the IP address ___.__.___.__ is Dennis -----. Furthermore, the representative of ---------- provided another Special Agent of the USSS at this agent's request with a Sun Microsystems Netra model computer, which is the Computer and which Dennis ----- had left at the facilities of ----------.

13. On or about March 10, 2005, another Special Agent of the USSS was contacted by the same ----- representative referred to in paragraph 9, above. The ----- representative indicated that there had been another intrusion into -----'s computer network in New York, New York, and that the records for customer accounts records had been accessed by one or more persons not authorized to access these account records. In addition, the ----- representative informed the other Special Agent of the USSS that the Internet Protocol ("IP") address associated with this unauthorized access was --.--.---.---.

14. Based on my review of documents and the conversations of another Special Agent of the USSS with a representative of Optimum Online, I determined that the ISP assigned to the IP address --.--.---.--- is CSC Incorporated, which, based on my experience, I am aware is an

ISP that does business under the trade name Optimum Online. Based on my review of documents and the conversations of another Special Agent of the USSS with a representative of Optimum Online, I determined that, on March 11, 2005, the Optimum Online customer assigned the IP address --.--.---.--- is Dennis ------, whose Optimum Online account address is ---- ---------- th Street, Apartment -, North Bergen, New Jersey 07047.

ITEMS TO BE SEIZED

15. Based upon my training, experience, and information obtained in the course of this and other investigations, I am familiar with the practices and methods of persons committing offenses such as unauthorized computer intrusions. Based on this, and the facts set forth above, I believe there is probable cause to believe that the Apartment and the Computer are likely to contain, among other things, documents, and materials referencing or regarding ---------- ----- & Co., persons or entities maintaining accounts at ---------- & Co., and the computer systems of ---------- ----- & Co., including any website maintained by ---------- & Co., and that the Apartment is likely to contain, among other things, computers and computing equipment. The items to be seized are set forth more fully in Attachment B.

METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS AND COMPUTER-RELATED EQUIPMENT

16. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation,

Distributed in Forward Edge II

and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the Apartment. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,024 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing sixty gigabytes of data are now commonplace in desktop computers. Consequently, each non-

Distributed in Forward Edge II

networked, desktop computer found during a search can easily contain the equivalent of 30 million pages of data, which, if printed out, would completely fill a 40' x 48' x 40' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

17. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant at the Apartment and the Computer, to the extent applicable, will employ the following procedure:

a. Upon securing the Apartment, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items contain contraband and whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

Distributed in Forward Edge II

b. If the computer equipment and storage devices cannot be searched on-site within a reasonable amount of time and without jeopardizing the ability to preserve the data, and if the computer equipment and storage devices do not contain contraband, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. If the computer personnel determine that these items contain contraband, or that it is not practical to perform an on-site search or make an on-site copy of the data, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

d. The analysis of electronically stored data, whether performed on-site or in a separate, controlled environment may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); "opening" or reading the first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "key-word" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

18. Any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not: (a) an instrumentality of the offense;

Distributed in Forward Edge II

(b) a fruit of the criminal activity; (c) contraband; (d) otherwise unlawfully possessed; or (e) evidence of the offense specified above.

a. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

b. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41 (b), the government will return these items, upon request, within a reasonable period of time.

Conclusion

19. Based upon the facts set forth herein, I believe, and respectfully submit that there is probable cause to believe, that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(2)(C), set forth more fully in Attachment B, are located at the Apartment and on the Computer.

Distributed in Forward Edge II

20. WHEREFORE, I respectfully request that a search warrant issue allowing Special Agents of the United States Secret Service, including computer technicians, to search the Apartment and the Computer, and to seize the items more fully set forth in Attachment B, including, but not limited to, computer or electronic records, documents, and materials referencing or regarding ---------- ----- & Co., persons or entities maintaining accounts at ---------- ----- & Co., and the computer systems of---------- ----- & Co., including any website maintained by ---------- ----- & Co.

_____
ROBERT B. AGENT, Special Agent
UNITED STATES SECRET SERVICE

Sworn to before me this
11th day of March, 2005

_____
____ THE HONORABLE IRMA
JUDGE, United States Magistrate
Judge

Distributed in Forward Edge II